

REMARKS

I. Status of Claims

The Applicant has carefully considered the Office Action dated October 15, 2008, the Advisory Action dated January 15, 2009, and the references cited therein. Currently, claims 1-12 are pending. In the Office Action, claims 1-5 and 7-10 were rejected under 35 U.S.C. § 103(a) as being obvious over 3rd Generation Partnership Project, "Document 2: KASUMI Specification" Release 4 (*DKS*) in view of U.S. Patent No. 6,324,288 (*Hoffman*) and in further view of "Parallel Stream Cipher for Secure High-Speed Communication" to Lee (*Lee*). Further, the Examiner objected to claims 6, 11, and 12 and indicated the claims would be allowable if rewritten in independent form to include the base claim and any intervening claims. In response, the Applicant submits the foregoing amendments and the following remarks.

II. Claim Rejections under 35 U.S.C. § 103(a)

Claim 1 recites an encryption method comprising, *inter alia*, performing the first-round of encryption by encrypting the received the first and second sub-bit streams with predetermined first encryption codes an odd number of times and outputting first and second ciphertext bit streams, generating a first operated ciphertext bit stream, generating a second operated ciphertext bit stream, and performing the second-round of encryption by encrypting the received first operated ciphertext bit stream and the second operated ciphertext bit stream with predetermined second encryption codes an odd number of times, wherein the last encryption for the second ciphertext bit stream in the first-round is performed at the same time of performing the first encryption of the first operated ciphertext bit stream in the second round of encryption.

The Applicants submit that the alleged combination of *DKS* and *Lee* does not describe a second round of encryption, wherein the wherein the last encryption for the second ciphertext bit stream in the first-round is performed at the same time of performing the first encryption of the first operated ciphertext bit stream in the second round of encryption. In particular, the Applicant notes that, in the Office Action, the Examiner contends that generating a first operated ciphertext and a second operated ciphertext is analogous to the FL function illustrated in FIG. 4 and described in 4.2 of *DKS*. As illustrated in FIG. 1 of *DKS*, the FL2 function depends on the result of FO2, which further depends on the FO1 and the

FL1 function. *See DKS at p. 18, FIG. 1.* Accordingly, the FL functions described in *DKS* are not analogous to claim 1, which recites the last encryption for the second ciphertext bit stream in the first-round is performed at the same time of performing the first encryption of the first operated ciphertext bit stream in the second round of encryption.

None of the cited prior art, either alone or in combination, cure the deficiencies of *DKS*. Thus, for at least the foregoing reasons, claim 1 and all claims depending therefrom are in condition for allowance and notice to that effect is respectfully requested. Independent claim 8 and all claims depending therefrom are also patentable for at least substantially the same reasons discussed above in connection with claim 1.

III. Conclusion

The Applicant submits that the above amendments and arguments are fully responsive to the Office Action dated October 15, 2008. Further, the Applicant submits that, for at least the foregoing reasons, all pending claims are in condition for allowance and notice to that effect is requested. Should the Examiner have any questions, the Examiner is encouraged to contact the undersigned at the telephone number indicated below.

Respectfully submitted,

A handwritten signature in black ink, appearing to read 'S. Booth', written over a horizontal line.

Simon Booth
Attorney of Record
Reg. No. 58,582

Roylance, Abrams, Berdo & Goodman, L.L.P.
1300 19th Street, N.W., Suite 600
Washington, D.C. 20036-2680
(202) 659-9076

Dated: February 11, 2009